ESCC
Enterprise Solutions Competency Center

U.S. ARMY
ENTERPRISE SOLUTIONS
COMPETENCY CENTER

Army Information Assurance (IA) Compliance Strategy Reference Guide

CHIEF INFORMATION OFFICE (CIO)
G-6
UNITED STATES ARMY

DROIT ET AVANT

Introduction

- The Army Information Assurance Program (AIAP) is a unified approach to protecting unclassified, sensitive, or classified information stored, processed, accessed, or transmitted by information systems.

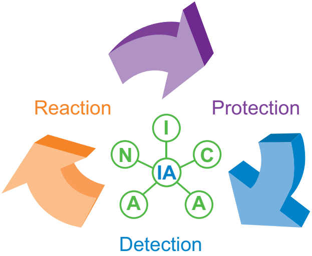
- It is established to consolidate and focus Army efforts for securing that information, including its associated systems and resources, to increase the level of trust in this information and its originating sources.

- **The purpose of this reference guide is to:**
  - Provide a general overview of IA
  - Provide the framework of the Army IA Compliance Model
  - Outline the framework of the Command IA team
  - Increase IA compliance awareness Army-wide.

What is IA?

IA includes measures that protect and defend information and information systems by ensuring their integrity, confidentiality, availability, authentication, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

IA Definition Model



Five Tenets of IA

Integrity

- Protection against unauthorized modification or destruction of information

Confidentiality

- Assurance that information is not disclosed to unauthorized individuals, processes, or devices

Availability

- Timely, reliable access to data and information services for authorized users

Authentication

- Security measures designed to establish the validity of a transmission, message, or originator

Non-repudiation

- Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data

Federal:

- Office of Management and Budget *Circular No. A-130*, Management of Federal Information Resources
- NSA/CSS Manual 130-1, *Operational Computer Security Manual*
- Federal Information Security Management Act of 2002, Title III — Information Security (Public Law 107-347)

Joint:

- Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510.01, August 15, 2007

DoD:

- Department of Defense Directive Number 8500.1, October 24, 2002
- Department of Defense Instruction Number 8500.2, February 6, 2003

Army:

- Army Regulation (AR) 25-1, *Army Knowledge Management and Information Technology*
- Army Regulation (AR) 25-2, *Information Assurance*
- Army Regulation (AR) 380-53, *Information Systems Security Monitoring*

Regulatory Requirements of IA

Importance of IA

- IA is a key enabler that protects the warfighter by securing and defending the Global Information Grid, which supports net-centric warfare, information superiority, decision superiority, and full spectrum dominance.

- As net-centric warfare and the cyber threat grows, IA compliance is critical to the success of worldwide Army operations and protection of the warfighter.

- “It is critical that Army leaders at all levels engage in the IA Compliance Strategy and enforce IA policy compliance and improve awareness across the total Army. Through our collective efforts, we must institutionalize IA into the Army’s culture.” — The Inspector General

- Lack of leader engagement:
  - Leads to lack of support for IA programs
- Insufficient funding and IA personnel to accomplish mission
- Lack of annual review of IA controls
- Emerging cyber threat
- Overall lack of user IA compliance awareness

Army IA Compliance Challenges

Critical Success Factors

- Increase leadership engagement
- Understand there is no quick panacea for IA compliance
- Require continuous IA program improvement to mitigate risk
- Tailor IA awareness to the mission of the unit

Myth: If my lockout screen has been set for 15 minutes but I can change it, then it's OK to set it for more than 15 minutes.

Fact: Army Regulation (AR) 25-2 states that after a maximum of 15 minutes, the organization's information system must automatically lock.

Myth: It's OK to have a wireless communications device (i.e. cell phone or PDA) in a secure area as long as I don't turn it on.

Fact: Army Regulation (AR) 25-2 and Army Regulation (AR) 380-5 prohibit portable electronic devices in areas where classified information is discussed or processed.

Myth: I don't need to worry about IA because my director of information management handles it.

Fact: False. IA is the responsibility of all users.

Myths and Facts

Myth: It's OK for me to bring my personal laptop and plug it into a government network.

Fact: The use of an employee-owned information system for ad-hoc (one-time or infrequent) processing of unclassified information is restricted and only permitted with the approval of an IA manager, designated approval authority, or commander. The use of employee-owned information systems to process classified or sensitive information is prohibited.

Myth: I can utilize my personal thumb drive on government information systems.

Fact: Only government-issued thumb drives with proper labeling and configuration with an approved data-at-rest solution are allowed on government systems.

Myth: Just opening an e-mail or an e-mail attachment can't harm my computer or the network.

Fact: Code embedded in an e-mail or attachment, if opened, can result in your computer or network being compromised. If you receive a suspicious e-mail, immediately notify your IA security officer or information management officer.

Myth: I only need to take IA awareness training once: when I first request my account.

Fact: IA awareness training must be conducted annually. IA is a dynamic environment, and the threat is always changing. It is important to stay abreast of recent threats.

Myths and Facts

Myth: I do not need to do a certification and accreditation (C&A) package because I'm under a Single Directorate of Information Management (DOIM), and it manages everything now.

Fact: All information systems will be certified and accredited in accordance with Army Regulation (AR) 25-2 and Department of Defense Instruction 8500.2 IA controls. Although tenant organizations may receive support under a Single DOIM, there are still C&A documentation requirements as indicated in the C&A Terms for Connection to the Installation Campus Area Network Best Business Practice.

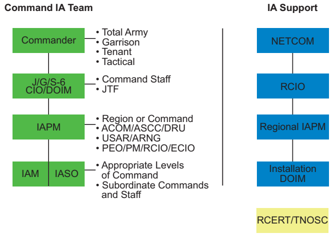
Myth: I have antivirus software and a firewall, so I'm safe.

Fact: Antivirus solutions require constant updates to recognize new attack patterns. As a result, brand new attacks may get through without the virus scanner even detecting it. A firewall reduces your exposure, but it doesn't eliminate it. Antivirus software and firewalls are essential components of an IA solution, but they do not provide complete protection.

Myth: The purpose of IA is to eliminate risk to our information systems.

Fact: Even if you do everything properly, you will never eliminate all risk. The purpose of the IA program is to reduce risk to an acceptable level. Patch your systems, reduce your exposure to the minimum level necessary to do business, remove or disable services and processes you do not require, do your backups (rotate them off-site), encrypt where necessary, develop recovery and continuity plans (test them annually), observe the principle of least privilege, maintain separation of duties, and secure your facilities. Then you'll be on your way to a manageable risk level.

IA Resource Structure



Command IA Team

Commander
- Total Army
- Garrison
- Tenant
- Tactical

J/G/S-6 CIO/DOIM
- Command Staff
- JTF

IAPM
- Region or Command
- ACOM/ASCC/DRU
- USAR/ARNG
- PEO/PM/RCIO/ECIO

IAM | IASO
- Appropriate Levels of Command
- Subordinate Commands and Staff

IA Support

NETCOM

RCIO

Regional IAPM

Installation DOIM

RCERT/TNOSC

- The Command IA team has the responsibility for meeting IA compliance requirements associated with the Command IA program.
- The Directorate of Information on Management (DOIM) is another resource available to the Command IA team and should be used as a first line of support for mitigating IA non-compliance matters. Additionally, the unit information management officer and DOIM are the first levels of support for the Command IA team to seek assistance in correcting non-compliant IA areas.
- The Command IA team should seek assistance from the regional CIO for additional expertise and resources.

Command IA Team

Commander:

- Commanders at various levels are in charge of the IA program for their respective commands
- Responsibilities found in Army Regulation (AR) 25-2, paragraphs 2-8, 2-25, and 3-2.

G/S-6:

- Is the principle staff officer with the responsibility for the management of the commander’s IA program in accordance with Field Manual 6-0, appendix D, paragraph D-76.

IA Program Manager:

- Appointed by commanders/director of Army Commands; Army Service Component Commands; Army Direct Reporting Units; U.S. Army Reserve; Army National Guard; Chief, CAR ; Program Executive Offices; direct reporting program manager; regional chief information officers/functional chief information offices; and the AASA as regional or command IA program management
- Accountable for establishing, managing, and assessing the effectiveness of all aspects of the IA program within a region, command, or functional activity
- Responsibilities found in Army Regulation (AR) 25-2, paragraph 3-2b

IA Manager:

- Appointed at all appropriate levels of command. This includes subordinate commands, posts, installations, and tactical units
- Enforces IA vulnerability management dissemination, reporting, compliance, and verification procedures
- Conducts security inspections, assessments, tests, and reviews
- Negotiates certification and accreditation issues with designated approving authorities
- Responsibilities found in Army Regulation (AR) 25-2, paragraph 3-2d

IA Security Officer:

- Appointed by commander or manager/director of activity responsible for each information system or group of information systems
- Ensures implementation of IA vulnerability management dissemination, reporting, and compliance procedures
- Ensures all users meet the requisite favorable security investigations, clearances, authorizations, and need-to-know and security responsibilities before granting access to the information system
- Ensures users receive initial and annual IA awareness training
- Responsibilities found in Army Regulation (AR) 25-2, paragraph 3-2f

IA Support Relationship

Regional Chief Information Officer:

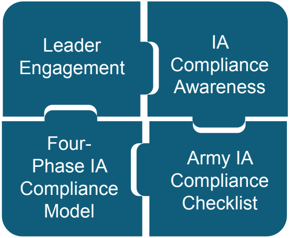
- Provides guidance for and ensures implementation of Army IA Program policy and procedures within his or her region
- Responsibilities found in Army Regulation (AR) 25-2, paragraphs 2-8 and 3-2

Director of Information Management:

- Implements an IA program as directed by the Garrison commander
- Ensures Army standards for connection to the ICAN are met
- Executes the certification and accreditation processes and obtains approval to operate the ICAN
- Responsibilities found in Army Regulation (AR) 25-2, paragraph 2-30

Designated Approval Authority:

- Vested with the authority to formally assume responsibility for operating an information system at an acceptable level of risk
- Responsibilities found in Army Regulation (AR) 25-2, paragraph 5-8



A compliance framework is pivotal as the Army focuses on the people, processes, and technology required to improve IA compliance across the Army.

Leader engagement:

- Socialization — change culture
- Compliance enablers
- Process/system improvement

IA compliance awareness:

- Strategic communications engagement
- Tells the IA story to Army stakeholders

Four-phase IA compliance model:

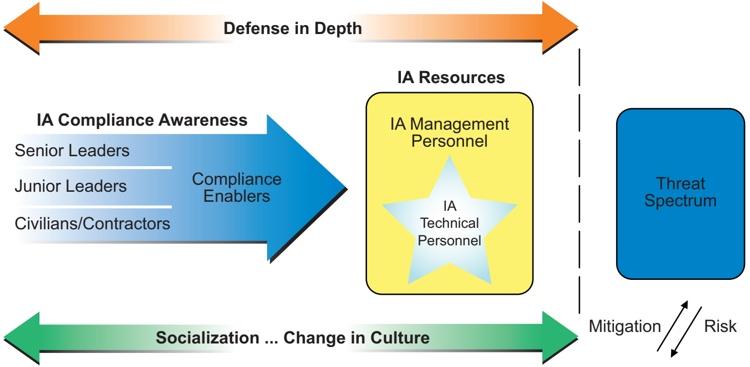
- Self-assessment virtual tool
- Resource de-confliction
- Focused, phased activities

Army IA compliance checklist:

- Baseline total army
- Establish IA program construct
- Authoritative standards

IA Compliance Framework

Leader Engagement



Improvement of an organization’s IA Compliance Posture requires leadership engagement. Leaders establish the culture of their organizations by their actions or lack thereof. Through increased IA compliance awareness, leaders at all levels can engage in the IA Compliance Strategy by becoming compliance enablers. The current IA threat environment is extremely complex and sophisticated. The threat is both internal (users) and external (recreational, professional, criminal, state/non-state sponsored). The resources employed to counter these threats and reduce the risks are both technical and non-technical. Risks imposed by threats can never be completely eliminated; however, increasing the level of IA compliance will minimize them. Leaders must actively support and engage in the IA Compliance Strategy through their involvement in appointing appropriate IA personnel and ensuring compliance standards are met within their organizations.

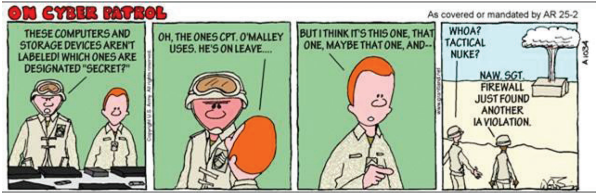
Leader Engagement

IA Compliance Awareness

IA compliance awareness is a continuous process. It's critical that we share lessons learned with both internal and external Army stakeholders. The chief information officer/G-6 has established IA professional awards for civilian and military personnel. There are additional ways to increase IA awareness such as:

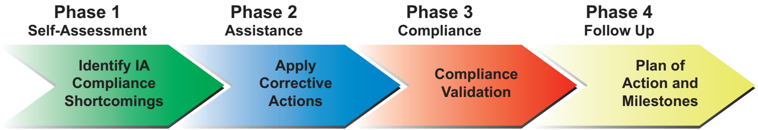
- Recognizing users/employees for good IA practices
- Publishing IA newsletters
- Attending IA-related conferences
- Infusing IA into professional military education

User IA awareness training and education programs can be found at: https://ia.gordon.army.mil.


ON CYBER PATROL
As covered or mandated by AR 25-2
THESE COMPUTERS AND STORAGE DEVICES AREN'T LABELED! WHICH ONES ARE DESIGNATED "SECRET?"
Copyright U.S. Army. All rights reserved.
OH, THE ONES CPT. O'MALLEY USES. HE'S ON LEAVE....
BUT I THINK IT'S THIS ONE, THAT ONE, MAYBE THAT ONE, AND--
www.grantland.net
WHOA? TACTICAL NUKE?
NAW, SGT. FIREWALL JUST FOUND ANOTHER IA VIOLATION.
A 1034

The Department of the Army Inspector General — Information Assurance Division, in coordination with the Office of the Chief Information Officer, has developed a four-phase IA compliance model for implementation across the Army.

The purpose of the four-phase model is to standardize IA compliance activities.



Phase 1
Self-Assessment

Identify IA Compliance Shortcomings

Phase 2
Assistance

Apply Corrective Actions

Phase 3
Compliance

Compliance Validation

Phase 4
Follow Up

Plan of Action and Milestones

Facilitates unity of effort across the total Army

Four-Phase IA Compliance Model

Phase 1 (Conduct IA Self-Assessment)

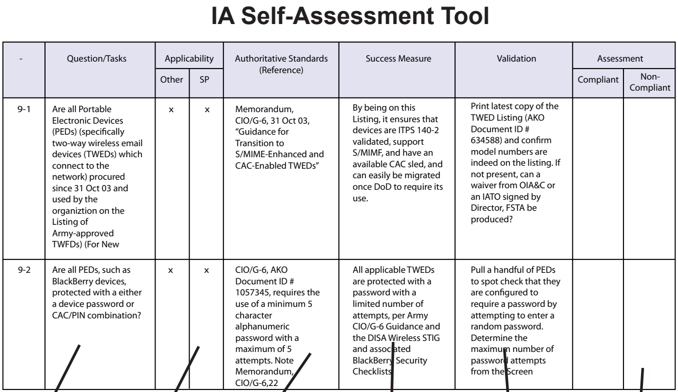
Self-assessment is the first step towards IA compliance. It is conducted by your G/S-6 or equivalent with support from IA staff.

Purpose:

- To identify IA compliance strengths and weaknesses
- To develop an improvement plan addressing identified weaknesses
- To prepare organizations for IA compliance inspections

The self-assessment tool is Web-based and can be found at the site below.

https://iatraining.us.army.mil



IA Self-Assessment Tool

-	Question/Tasks	Applicability		Authoritative Standards (Reference)	Success Measure	Validation	Assessment	
		Other	SP				Compliant	Non-Compliant
9-1	Are all Portable Electronic Devices (PEDs) (specifically two-way wireless email devices (TWEDs) which connect to the network) procured since 31 Oct 03 and used by the organiztion on the Listing of Army-approved TWFDs) (For New	x	x	Memorandum, CIO/G-6, 31 Oct 03, "Guidance for Transition to S/MIME-Enhanced and CAC-Enabled TWEDs"	By being on this Listing, it ensures that devices are ITPS 140-2 validated, support S/MIMF, and have an available CAC sled, and can easily be migrated once DoD to require its use.	Print latest copy of the TWED Listing (AKO Document ID # 634588) and confirm model numbers are indeed on the listing. If not present, can a waiver from OIA&C or an IATO signed by Director, FSTA be produced?		
9-2	Are all PEDs, such as BlackBerry devices, protected with a either a device password or CAC/PIN combination?	x	x	CIO/G-6, AKO Document ID # 1057345, requires the use of a minimum 5 character alphanumeric password with a maximum of 5 attempts. Note Memorandum, CIO/G-6,22	All applicable TWEDs are protected with a password with a limited number of attempts, per Army CIO/G-6 Guidance and the DISA Wireless STIG and associated BlackBerry Security Checklists	Pull a handful of PEDs to spot check that they are configured to require a password by attempting to enter a random password. Determine the maximum number of password attempts from the Screen		

Question

Applicability

Standard

Success Measure

Validation

Assessment

Used by leadership as an executive management tool

IA Self-Assessment Tool

Benefits of using the self-assessment tool:

- Identifies IA compliance strengths and weaknesses
- Establishes the framework for the Command IA Compliance Improvement Plan
- Prepares an organization for an IA compliance inspection
- Increases IA compliance awareness
- Reinforces the framework for the Command IA team
- Consists of 15 functional areas (addressed in the next section)
- Provides an organization with authoritative IA standards and policy

The self-assessment tool is applicable to the total Army:

- Active Army
- Army National Guard
- U.S. Army Reserve
- Program executive officers
- Direct reporting program managers
- Strategic, tactical, and non-tactical environments or installations

For questions concerning the IA self-assessment tool, please e-mail: netcom-iasat@hqda.army.mil.

Phase 2 (Assistance)

- During Phase 2, the Command IA team should focus on applying corrective actions to IA compliance shortcomings noted during the IA self-assessment (Phase 1).

- Tools available to the Command IA team:
  - Establish an IA compliance awareness program
  - Request IA staff assistance visits
  - Review IA functional area shortcomings during staff meetings.

Coach Teach and Train

Phase 3 (Compliance Validation)

- Compliance inspections will be conducted using the Army IA compliance checklist.

- The Army IA compliance checklist is the only checklist used by the Department of the Army Inspector General — IA (DAIG-IA) for compliance/validation inspections:
  - The checklist defines IA focus and non-focus areas
  - Findings from the compliance/validation process are briefed by the DAIG-IA to Army senior leadership.

- Modifications and revisions to the checklist are determined by the IA Compliance Configuration Control Board.

- The checklist is available at the following site: https//www.us.army.mil/suite/page/475521 or from the command IG.

Phase 4 (Follow-Up)

IA Compliance Plan of Action and Milestones (POA&M)

Army IA Compliance POA&M

Functional Area	Question	Description of Vulnerability/Shortfall	Operational Impact	Recommended Solution	Remediation Action Taken or ECD	Status	Last Status Update	Update Due to DAIG	Suspense Date
IA Program Management	**4**	**The Disaster Recovery Plan is not fully developed**	**Lack of clear restoration instructions could result in an unacceptable gap in critical services**	**Develop and promulgate a Disaster Recovery Plan**	**20-Nov-07**	**Open**	**2-Aug-07**	**1-Sep-07**	**2-Dec-07**

The IA Compliance POA&M Model was developed by the Department of the Army Inspector General — IA to be used during phase four of the four-phase IA compliance model. The IA compliance POA&M helps to identify all non-compliance findings discovered during the phase three compliance inspection. The POA&M provides the commander with the operational impact of the finding, recommendations for a solution, and a timeline for correcting each non-compliance finding.

The Command IA team is responsible for executing recommended solutions outlined in the IA Compliance POA&M.

Army IA Compliance Checklist

The Army IA compliance checklist is a compliance validation tool. It is comprised of IA functional areas that represent the major activities for the Command IA program.

The list of IA checklist functional areas is similar to the IA self-assessment tool. The checklist is an evolutionary tool with approval of major revisions made by the IA Compliance Configuration Control Board.

A general overview and required actions are listed for each functional area. A more detailed list of compliance standards is available at the IA self-assessment tool and IA compliance checklist.

Checklist

1. Incident handling
2. IA training and certification
3. IA vulnerability management
4. IA program management
5. Public key infrastructure
6. Certification and accreditation
7. Federal information security
8. Management Act wireless security
9. Portable electronic device
10. Army Web risk content management
11. Personal identifiable information protection
12. Minimum IA technical requirements
13. Classified systems management
14. Communications security
15. *Leadership IA assessment

*The leadership IA assessment is only used in the IA self-assessment tool

Army IA Functional Areas

Incident Handling

Overview:

- Incident handling deals with the actions you perform subsequent to identifying an incident. These actions will not only affect your organization’s operations but may impact future procedures, your security posture, and the outcome of the situation. Incident handling procedures pertain to all individuals with access to, or who are responsible for managing, Army assets.

Actions:

- Commands will establish an incident response plan and an incident response team
- Train users on incident handling procedures
- Establish procedures for handling classified information spillage

IA Training and Certification

Overview:

- The Department of Defense has mandated that all personnel performing IA duties will be trained and certified according to their positions.

Actions:

- All general users with network access must receive initial and annual computer security awareness training.
- IA certification programs will produce IA personnel with the demonstrated ability to perform the functions of their assigned positions.

IA Vulnerability Management (IAVM)

Overview:

- Vulnerabilities, if left undetected, often pose a serious security risk to enterprise systems and can leave your vital data exposed to malicious attacks. Some risks include possible extended system downtimes and loss of revenue and productivity.

Actions:

- Command IA team will ensure all units and organizations report IAVM compliance status of their assets in the Army Asset and Vulnerability Tracking Resource.
- Command IA team will identify devices on its network that are open to known vulnerabilities and remediate them. If unable to comply, the team will submit a Plan of Action and Milestones approved by its designated approval authority.

IA Program Management

Overview:

- An effective IA program is needed to ensure that the Department of the Army's information, information systems, and information infrastructure remain secure. Army Regulation (AR) 25-2 is the foundational document that senior managers use to develop their IA programs.

Actions:

- Commanders will ensure that an IA personnel structure is established.
- Command IA team will establish a contingency plan for critical assets.
- Enable conditions for compliance with IA policy and guidance.

Public Key Infrastructure

Overview:

- The framework was established to issue, maintain, and revoke public key certificates accommodating a variety of security technologies, including the use of software.

Actions:

- The command IA team will ensure that all NIPRNET workstations are public key enabled.
- The command IA team will ensure that all system administrators are using their Common Access Cards or Alternative Smart Card Logon tokens to access their higher-privileged accounts.

Certification and Accreditation

Overview:

- The certification and accreditation (C&A) process ultimately determines whether information systems are authorized to operate under present conditions. Upon reviewing C&A documentation, the designated approval authority (DAA) will decide whether risks to the system are at an acceptable level. The DAA will then issue an Approval to Operate, Interim Approval to Operate (ATO), or Interim Approval to Test.

Actions:

- Ensure that the re-accreditation process begins at least one year from the ATO expiration.
- Ensure that a Department of Defense (DoD) IA C&A process transition plan has been developed for moving each information system from the Information Technology Security C&A Process to the DoD IA C&A Process.

Federal Information Security Management Act (FISMA)

Overview:

- FISMA is the foundation for the command IA program and Department of Defense’s IA scorecard that is reportable to Congress.

Actions:

- Ensure that all systems requiring accreditation have a valid accreditation Approval to Operate (ATO).
- Commander will ensure that security controls are tested annually, IA training certification is conducted and documented, and that ATO, Interim Approval to Operate, or Interim Approval to Test are identified in the Army Portfolio Management System.

Wireless Security

Overview:

- Wireless infrastructures lack the physical security limitations inherent in wired infrastructures. Radio frequencies can penetrate walls allowing connectivity (and increased potential for network attacks) to occur from outside of the protected space.

Actions:

- Conduct wireless discovery scans at least monthly
- Ensure that wireless intrusion detection systems are utilized on a 24/7 basis to detect unauthorized wireless devices

Portable Electronic Devices (PEDs)

Overview:

- PEDs are designed to increase efficiency and make work possible in a variety of locations and include devices such as a laptop, BlackBerry, cell phone, USB drive, etc.

Actions:

- Ensure that all PEDs are protected with a five-character minimum alphanumeric password.
- Ensure that laptops and other PEDs authorized for travel are properly configured for the Army approved data-at-rest solution.
- Ensure that no unauthorized PEDs (i.e. Bluetooth devices) are being used on Army networks.

Army Web Risk Content Management

Overview:

- Use of the Internet is vital to operations, but risks are inherent due to ease of access. It is critical that content on the Web be managed to ensure that sensitive information is not at risk. The Army Web Risk Assessment Cell (AWRAC) is designed to review content on the Web.

Actions:

- Ensure that AWRAC assessments are requested for publically available official ".army.mil" Web sites
- Ensure that inappropriate security and personal information is removed from publicly accessible Web sites
- Ensure publically accessible Web sites are behind an Army Reverse Proxy Server
- Have a designated reviewer conduct quarterly (routine) reviews of Web sites

Personally Identifiable Information (PII) Protection

Overview:

- PII is any piece of information that potentially can be used to uniquely identify, contact, or locate a single person. This includes such information as Social Security number, address, financial records, blood type, etc.

Actions:

- Establish policies and procedures for protecting and reporting the loss of PII.

Minimum IA Technical Requirements

Overview:

- Outline and design responsibilities for achieving acceptable levels of IA in engineering, implementation, operation, and maintenance for all information systems connecting to or crossing any Army managed network

Actions:

- Develop, disseminate, periodically review/update, and enforce formal documented access control policy.
- Properly manage the establishment, activation, modification, review, disablement, and removal of system accounts.

Classified Systems Management

Overview:

− Classified systems carry information that will cause varying degrees of damage to the mission if mishandled.

Actions:

− Commander will establish procedures for:
  - Sanitizing and destroying media
  - Physically storing documents
  - Labeling processing equipment.

Communications Security (COMSEC)

Overview:

- Measures and controls taken to deny unauthorized individuals access to information derived from telecommunications and to ensure the authenticity of such telecommunications. COMSEC includes crypto security, transmission security, emission security, and physical security of COMSEC material.

Actions:

- Appoint and train a COMSEC custodian to manage COMSEC assets.

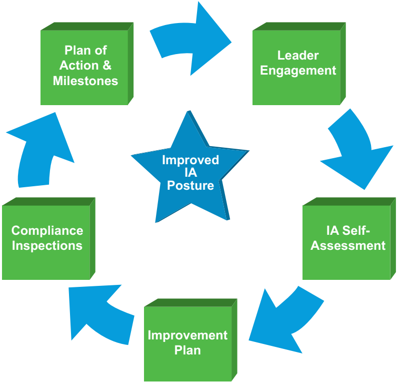
Leadership IA Assessment

Overview:

- The success of the Command IA program begins and ends with the leader. The more leaders understand and champion compliance, the better the IA posture will be.

Actions:

- Understand the Command IA team structure and your IA responsibilities.
- Ensure that IA personnel are equipped with funding and resources to achieve IA success.
- Continue full support of IA.



Step 1: Leader Engagement

- Leaders are compliance enablers; they shape and form the culture of their organizations by their actions.
- Without leadership engagement, the IA program will not succeed.

Sustained IA Compliance

Sustained IA Compliance

Step 2: IA Self-Assessment

- Conducting IA self-assessment is the most critical phase of the IA compliance strategy.
- Assessment should be done regularly due to changes in policy, personnel departures, and emerging threats/technology.

Step 3: Improvement Plan

- Compliance shortcomings from the self-assessment are addressed in the improvement plan.
- Coordinate with your IA staff, Command inspector general and regional IA support structure to assist correcting non-compliant areas.

Step 4: Compliance Inspections

- Rigorous inspections will be conducted to analyze IA compliance.
- Assist with the validation of the commands self-assessment.

Step 5: Plan of Action & Milestone (POA&M)

- The POA&M will be used to outline a timetable for improving weaknesses found after the compliance inspection.

IA Compliance Begins and Ends With YOU!

When it comes to IA threats, there is no panacea. Threats to IA as well as technology, personnel, leadership, policy, and other aspects of the IA posture change rapidly. That is why IA must be regarded as a continuous process. There is no one-time fix. It takes the efforts of everyone to maintain a healthy IA posture. Program managers should continuously assess their programs, IA professionals need to use their expertise to assist others, end users must comply with policies, and leaders must be engaged and vigilant in improving IA compliance throughout the Army. In today’s net-centric world, IA compliance is more important than ever and not only protects information but also the lives of soldiers fighting for our freedom.

Definitions

Accreditation − Formal declaration by a designated accrediting authority that an information system (IS) is approved to operate at an acceptable level of risk based on the implementation of an approved set of technical, managerial, and procedural safeguards (see security safeguards).

Certification − Comprehensive evaluation of the technical and nontechnical security safeguards of an IS to support the accreditation process that establishes the extent to which a particular design and implementation meets a set of specified security requirements.

Countermeasure − An action, device, procedure, technique, or other measure that reduces the vulnerability of an IS.

Data security − Protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure.

Defense in depth − IA strategy integrating people, technology, and operational capabilities to establish variable barriers across multiple layers and dimensions of networks — synonymous with security-in-depth.

Designated Approval Authority − Official with the authority to formally assume responsibility for operating an information system (IS) or network at an acceptable level of risk.

Department of Defense Information Assurance Certification and Accreditation Process − All systems for which the principal Headquarters, Department of the Army office is the system owner are accredited, annually revalidated, and re-accredited in accordance with Department of Defense IA Certification and Accreditation Process.

Event − Occurrence, not yet assessed, that may affect the performance of an IS.

Incident − Assessed occurrence having actual or potentially adverse effects on an information system (IS).

Information assurance − Measures that protect and defend information and ISs by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of ISs by incorporating protection, detection, and reaction capabilities.

Information Assurance Vulnerability Management (IAVM) − IAVM is the Department of Defense program to identify and resolve identified vulnerabilities in operating systems. It requires the completion of four distinct phases to ensure compliance.

Network security − Protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats.

Public key infrastructure − Framework established to issue, maintain, and revoke public key certificates accommodating a variety of security technologies, including the use of software.

Risk − Possibility that a particular threat will adversely impact an information system (IS) by exploiting a particular vulnerability.

Risk assessment − Process of analyzing threats to and vulnerabilities of an IS and the potential impact resulting from the loss of information or capabilities of a system. This analysis is used as a basis for identifying appropriate and cost-effective security countermeasures.

Definitions

Threat − Any circumstance or event with the potential to impact an information system (IS) adversely through unauthorized access, destruction, disclosure, modification, or of data and/or denial of service.

Vulnerability − Weakness in an IS, system security procedures, internal controls, or implementation that could be exploited.

Vulnerability assessment − Formal description and evaluation of vulnerabilities of an IS.

Army Information Assurance, https://informationassurance.us.army.mil

Fort Gordon IA Training, https://ia.gordon.army.mil

Site for Self-Assessment Tool, https://iatraining.us.army.mil

Army Knowledge Online, https://www.us.army.mil

https://www.us.army.mil/suite/page/475521

DISA Information Assurance Support Environment, http://iase.disa.mil/policy-guidance/index.html

Joint Task Force Network Operations, https://www.jtfgno.mil/

DISA Security Technical Implementation Guides and Supporting Documents, http://iase.disa.mil/stigs/

ACERT Army Emergency Response Team,
https://www.acert.1stiocmd.army.mil/

References

- Army Regulation (AR) 25-1, *Army Knowledge Management and Information Technology*, July 15, 2005
- Army Regulation (AR) 25–2, *Information Assurance*, October 24, 2007
- Department of Defense Directive 8500.01E, *Information Assurance (IA)*, April 23, 2007
- Department of Defense Instruction 8500.2, *Information Assurance (IA) Implementation*, February 6, 2003
- Department of Defense Directive 8570.01, *Information Assurance Training, Certification, and Workforce Management*, April 23, 2007
- Department of Defense Manual 8570.01-M, *Information Assurance Workforce Improvement Program*, December 19, 2005
- *Information Assurance Compliance Strategy Implementation Guidance,* memorandum, October 22, 2007

Department of the Army Inspector General Agency
Information Assurance Division
2530 Crystal Drive, Suite 3172
Arlington, VA 22202
(703) 602-8674

Office of Information Assurance and Compliance
2530 Crystal Drive, 6th Floor
Arlington, VA 22202
(703) 602-7516

U.S. ARMY ENTERPRISE SOLUTIONS COMPETENCY CENTER

ESCC

Enterprise Solutions Competency Center

0308_TA_LT_1000

http://escc.army.mil

ESCC • 6000 6th St., S302 • Ft. Belvoir, VA 22060 • chip.raymond@us.army.mil